Commonwealth of Massachusetts
Executive Office of Technology Services and Security (EOTSS)
Enterprise Security Office

Compliance Standard

Document Name: Compliance	Effective Date: October 15th, 2018
Document ID: IS.007	Last Revised Date: August 29, 2022

Table of contents

1. PURPOSE

1.1. **Compliance —** This **standard** defines the requirements to ensure that the Commonwealth complies with all relevant legislative, regulatory, statutory and contractual requirements related to information security.

2. AUTHORITY

2.1. M.G.L. Ch. 7d provides that "Notwithstanding any general or special law, rule, regulation, executive order, policy or procedure to the contrary, all executive department agencies shall, and other state agencies may, adhere to the policies, procedures and objectives established by the executive office of technology services and security with respect to activities concerning information technology."

3. SCOPE

3.1. This document applies to the use of information, information systems, electronic and computing devices, applications, and network resources used to conduct business on behalf of the Commonwealth. The document applies to the Executive Department including all executive offices, and all boards, commissions, agencies, departments, divisions, councils, and bureaus. Other Commonwealth entities that voluntarily use or participate in services provided by the Executive Office of Technology Services and Security, such as mass.gov, must agree to comply with this document as a condition of use.   Executive Department agencies and offices are required to implement procedures that ensure their *personnel* comply with the requirements herein to safeguard information.

4. RESPONSIBILITY

4.1.   The Enterprise Security Office is responsible for the development and ongoing maintenance of this *standard*.

4.2.   The Enterprise Security Office is responsible this *standard* and may enlist other departments to assist with the monitoring and maintenance of compliance with this *standard*.

4.3.   Any inquiries or comments regarding this *standard* shall be submitted to the Enterprise Security Office by sending an email to EOTSS-DL-Security Office.

4.4.   Additional *information* regarding this *standard* and its related standards may be found at https://www.mass.gov/cybersecurity/policies.

5. COMPLIANCE

5.1. Compliance with this document is mandatory for all the Executive Department including all executive offices, boards, commissions, agencies, departments, divisions, councils, and bureaus. Violations are subject to disciplinary action in accordance to applicable employment and collective bargaining agreements, up to and including the termination of their employment and/or assignment with the Commonwealth.

Exceptions to any part of this document must be requested via email to the Security Office (EOTSS-DL-Security Office). A policy exception may be granted only if the benefits of the exception outweigh the increased risks, as determined by the Commonwealth CISO.

6. STANDARD STATEMENTS

6.1 Compliance with Policies, Standards, Guidelines and Procedures

The Enterprise Security Office shall ensure information enterprise security policies, standards, guidelines and procedures (PSGPs) are in place, communicated, implemented and enforced. The Information Security Team or Internal Audit shall conduct periodic assessments and reviews for compliance with PSGPs.

6.1.1 The Enterprise Security Office shall ensure information security PSGPs are in place, communicated, implemented, and enforced. Leading information security industry standards shall serve as guidance when developing and updating PSGPs.

6.1.2 The Commonwealth Chief Information Security Officer (CISO), Commonwealth Chief Risk Officer (CRO), and the EOTSS General Counsel (GC) shall be aware of and ensure that all relevant regulatory requirements are met. The EOTSS Security Team shall use global information security industry standards to serve as guidance when developing and updating the PSGPs.

6.1.3 The Commonwealth CISO and Commonwealth SOC shall perform or contract periodic assessments and reviews for compliance with IS PSGPs and applicable regulations.

6.1.4 The Commonwealth CISO and Commonwealth CRO team shall ensure compliance deficiencies identified during compliance reviews are remediated by the responsible Executive Office or Agency. Commonwealth Executive Offices and Agencies will in turn ensure that their **Information Owner** or **Information Custodian** work to remediate and rectify any gaps in compliance.

6.1.5 The **Information Owner,** in collaboration with the Enterprise Security Office (as needed), shall complete all regulatory reporting or audits to meet as required. This includes compliance with all relevant Massachusetts laws as well as federal and commercial compliance requirements including Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), Criminal Justice Information Services (CJIS) Security Policy, federal tax information (FTI) and others.

6.1.6 Reporting frequency shall be strictly respected.

6.2 Reporting Security Incidents and Violations

6.2.1 Commonwealth Executive Offices and Agencies must ensure that Commonwealth personnel are responsible for knowing and complying with applicable information security requirements.

6.2.2 Commonwealth Executive Offices and Agencies must ensure that potential violations shall be reported to an immediate supervisor or to the Enterprise Security Office at ITD-DL- MassIT - Compliance. Failure to report a violation is itself a violation.

6.2.3 Personnel who for any reason do not wish to discuss the problem directly may refer their concerns to their Human Resources (HR) representative.

6.2.4 Personnel will not be retaliated against for any good-faith complaint or violation report.

6.2.5   Information related to data breaches, incidents and investigations shall be managed and communicated in accordance with the *Information Security Incident Management* Standard.

6.3 Security Compliance Reviews

Information security risks that could compromise the confidentiality, integrity or availability of the Commonwealth's **information assets** shall be identified, analyzed and mitigated to an acceptable level to meet organizational objectives and compliance requirements.

6.3.1   The Commonwealth shall adopt a structured approach for assessing IS risks, identifying threats and vulnerabilities and implementing mitigation strategies (see *IS.010 Information Security Risk Management Standard).*

6.3.2   The Commonwealth CISO shall develop, disseminate and review annually a formal, documented security review and accountability plan, with specific review and accountability goals, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and formal, documented procedures to facilitate the implementation of the review and accountability plan and associated review and accountability controls.

6.3.3   Controls to safeguard operational systems and audit tools during information systems reviews shall be implemented.

6.3.3.1   Monitoring on mission-critical or high-risk systems must be persistent, and controls shall be implemented to tamper-proof the supporting log collection and analysis mechanisms.

6.3.3.2   The Enterprise Security Office shall use **log** harvesting, parsing and alerting tools to help facilitate the identification of **log** events that need to be reviewed (see *Log Review and Reporting* in the *Logging and Event Monitoring Standard*).

6.3.3.3   Audit logs must be retained in accordance with the log retention requirements (see the *Logging and Event Monitoring Standard*).

6.3.4   Review of audit events

6.3.4.1   The Commonwealth shall implement hardware, software, applications and services that shall have the capability of creating audit records containing security events in accordance with logging and monitoring procedures.

6.3.4.2   The Commonwealth SOC, in coordination with the CISO and CRO shall review and update at a minimum annually the listing of security events to be audited. **Information assets** owned by the Commonwealth that log security events shall have their security logging capability operational at all times.

6.3.4.3   The Commonwealth SOC, in coordination with the EOTSS and Secretariat Operations teams as appropriate, shall employ technology innovation to develop a capability to automate the storage and analysis of security audit records and reduce audit report generation. Audit records for security events of interest based on event criteria shall be analyzed by automated systems. The systems shall also be able to process ad hoc queries of security events.

6.4 External Attestation of Compliance

The Commonwealth may employ a third party to conduct external attestation or agreed-upon procedure examinations ("Attestation Engagements") for specific Commonwealth agencies.

Attestation Engagements are designed to provide reasonable assurance that a set of predefined trust principles, which address the information security risks of functions and processes, are achieved, and that the Commonwealth is equipped to effectively control these risks where they may exist in systems.

6.4.1 Attestation engagements

On an annual basis or as a result of a material change to the organization, the Commonwealth CISO, in consultation with the CRO, shall develop as part of the annual security plan a process that initiates independent reviews (e.g., penetration tests, audits and assessments) of Information Security.

The third party may evaluate Commonwealth systems based on the following principles and criteria, as applicable:

6.4.1.1 Security: the system is reasonably designed and operated to be protected against unauthorized access (both physical and logical).

6.4.1.2 Availability: the system is reasonably designed and operated to be available for operation and use as committed or agreed.

6.4.1.3 Processing integrity: the system processing is reasonably designed and operated to be complete, accurate, timely and authorized.

6.4.1.4 Confidentiality: there are reasonable steps taken to protect confidential consistent with applicable Commonwealth policies or to which otherwise agreed, including access by personnel.

6.4.1.5 Privacy: where applicable, privacy policies and procedures are defined and documented.

6.4.2 Attestation engagements shall be specific to the Commonwealth agency being tested and may include different criteria across agencies. The third party shall work with Commonwealth agencies individually to determine the appropriate principles and criteria for the specific examination.

6.4.2.1 Prior to undertaking any engagement, all third parties must sign confidentiality agreements and agreements covering their services, and steps must be taken by the relevant agencies in accordance with the *Third Party Information Security Policy* and other criteria the requesting agency may deem necessary.

6.4.3 Attestation engagement testing results shall be:

6.4.3.1 Recorded and reported to Information Owners, agency management; and as appropriate the Risk Governance Committee. Report shall include an update on the lifecycle of the mitigation plans for identified risks.

6.4.3.2 Maintained consistent with the records retention requirements.

6.4.4 Oversight and organization: Commonwealth agencies shall oversee the schedule of Attestation Engagements for their respective agency, coordinate with the third party to begin relevant engagements, and track the progress of engagements as they occur. Results shall be reported to the CISO, CRO, and relevant parties.

6.4.5 Engagement scoping: In scoping the engagement, the Commonwealth agency shall clearly establish the boundaries of what is to be assessed. As part of the scoping, ownership of each system, function or process under review must be clearly established so the assessment remains in scope and the correct individuals are identified to provide any required information. Agencies shall take into account that the results of Attestation Engagements may be for external distribution, unlike internal audits.

6.4.6 Storage and distribution:

6.4.6.1 Commonwealth agencies shall securely store and maintain the full results of their Attestation Engagements, and the CISO team shall securely store and maintain copies of all agency Attestation Engagements.

6.4.6.2 The results of external Attestation Engagements may be shared with Commonwealth stakeholders, including external entities that wish to gain an understanding and assurance of the security and integrity of the respective agencies and functions, and the efficacy of controls in place to reduce risks, should they exist.

6.4.6.3 Any decision to distribute Attestation Engagements results to external entities shall be made in consultation with Legal to address, among other things, any attorney-client privilege protections and requirements for non-disclosure agreements prior to distributing the results to the requestor.

7. CONTROL MAPPING

Section	NIST SP800-53 R5	CIS 18 v8	NIST CSF
6.1 Compliance with policies, standards, guidelines and procedures		-	PR.AC-1
		-	ID.RA-1
		-	ID.RA-1
		-	PR.AC-1
	PE-8	-	-
		-	-
6.2 Reporting security incidents and violations		-	PR.PT-1
		-	ID.GV-1
	IR-6	CSC 17	RS.CO-2
		-	ID.RA-1
		-	ID.RA-1
		-	ID.RA-1
		-	-
6.3 Security compliance reviews	RA-3	CSC 16	ID.RA-1
	CA-2	-	ID.RA-1
	CA-7	CSC 3	ID.RA-1
		-	ID.RA-1
	AU-6	CSC 8	PR.IP-7
6.4 External attestation of compliance		-	PR.AC-1
		-	PR.DS-5
		-	PR.AC-1
	CA-2	-	ID.RA-1
	CA-7	CSC 3	ID.RA-1
		-	-
		-	-
		-	ID.GV-1
		-	PR.PT-1
		-	PR.PT-1
	AC-20	-	ID.AM-4

8. RELATED DOCUMENTS

Document	Effective date

9. DOCUMENT CHANGE CONTROL

Version No.	Revised by	Effective date	Description of changes
0.90	Jim Cusson	10/01/2017	Corrections and formatting
0.92	John Merto	01/02/2018	Corrections, Formatting
0.95	Sean Vinck	5/7/2018	Corrections and Formatting
0.96	Andrew Rudder	5/31/2018	Corrections and Formatting
0.98	Anthony O'Neill	05/31/2018	Corrections and Formatting
1.0	Dennis McDermitt	06/01/2018	Pre-Publication Review
1.0	Andrew Rudder	10/4/2018	Approved for Publication by: John Merto
1.1	Megan Perkins	7/15/2020	Annual Review; Minor corrections and formatting
1.2	Sean M. Hughes	11/04/2021	Annual Review
1.3	Sean M. Hughes	08/29/2022	NIST 800-53r5 Mapping and Annual Review

The owner of this document is the Commonwealth CISO (and or his designee). It is the responsibility of the document owner to maintain, update and communicate the content of this document. Questions or suggestions for improvement should be submitted to the document owner.

9.1 Annual Review

This *Compliance Standard* should be reviewed and updated by the document owner on an annual basis or when significant policy or procedure changes necessitate an amendment.